

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No.

3:14mj-247

INFORMATION ASSOCIATED WITH)
"XIAFENMAIL@YAHOO.COM" THAT IS STORED AT)
PREMISES CONTROLLED BY YAHOO)

SHARON L. OVINGTON

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California (identify the person or describe property to be searched and give its location):

SEE ATTACHMENT A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of SEE ATTCH C U.S.C. § SEE ATTCH C, and the application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA ERIC M. PROUDFOOT, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

6-12-14

Judge's signature

City and state: DAYTON, OHIO

SHARON L. OVINGTON, U.S. MAGISTRATE JUDGE

Printed name and title

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with "XIAFENMAIL@YAHOO.COM" that is presently stored at premises owned, maintained, controlled, or operated by YAHOO! INC., a company headquartered at 701 First Avenue, San Jose, California 94089, Telephone (408) 349-5400, Facsimile (408) 349-7941.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by YAHOO!

To the extent that the information described in Attachment A is within the possession, custody, or control of YAHOO!, YAHOO! is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails stored in the account, including copies of emails sent from the account, e-mail saved in draft folders, e-mail placed in trash or deleted folders that have not yet been purged;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternate e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists; including but not limited to any pictures and files;
- d. All records pertaining to communications between YAHOO! and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the statutes listed on the warrant involving

XIAFENMAIL@YAHOO.COM since April 01, 2012, until the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. 18 U.S.C. § 641 - Theft of public money, property, or records.
- b. 18 U.S.C. § 666 – Theft concerning programs receiving Federal funds.
- c. 18 U.S.C. § 951 – Agents of a foreign governments.
- d. 18 U.S.C. § 953 – Private correspondence with foreign governments.
- e. 18 U.S.C. § 1343 – Wire fraud.
- f. 18 U.S.C. § 1349 – Conspiracy to commit wire fraud.
- g. 18 U.S.C. § 371 – General conspiracy.
- h. Records relating to who created, used, or communicated with the account identifier.

ATTACHMENT C

18 U.S.C. § 641	Theft of public money, property, or records
18 U.S.C. § 666	Theft concerning programs receiving Federal funds
18 U.S.C. § 951	Agents of a foreign governments
18 U.S.C. § 953	Private correspondence with foreign governments
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 1349	Conspiracy to commit wire fraud
18 U.S.C. § 371	General conspiracy

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Eric M. Proudfoot, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant seeking information associated with certain email accounts that are stored at premises owned, maintained, controlled, or operated by YAHOO!, an email service provider headquartered at 701 First Avenue, San Jose, California, 94089, telephone number (408) 349-5400, facsimile number (408) 349-7941. The specific information to be searched is described in the following paragraphs and in Attachment A. This supporting affidavit is submitted pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) and seeks to require YAHOO! to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.
2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since March 2, 2008. I have investigated Federal criminal violations related to the use of computers and computer-based crimes. I have received formal training in the investigation of these matters at the FBI Academy, and through subsequent in-service training, seminars and conferences. Prior to my employment with the Federal Bureau of Investigation, I served on active duty as an officer in the United States Air Force for six years. As a Federal Agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.
3. The facts in this affidavit have been gleaned from my personal observations, my training and experience, and information obtained from other Agents, law enforcement officers, and

witnesses. This affidavit is intended to merely show that there is sufficient probable cause for the issuance of the requested warrant and does not set forth all of my knowledge about this case.

STATUTORY AUTHORITY

4. This affidavit is based on alleged violations of the following criminal statutes:
 - a. 18 U.S.C. § 641 - Theft of public money, property, or records.
 - b. 18 U.S.C. § 666 – Theft concerning programs receiving Federal funds.
 - c. 18 U.S.C. § 951 – Agents of a foreign governments.
 - d. 18 U.S.C. § 953 – Private correspondence with foreign governments.
 - e. 18 U.S.C. § 1343 – Wire fraud.
 - f. 18 U.S.C. § 1349 – Conspiracy to commit wire fraud.
 - g. 18 U.S.C. § 371 – General conspiracy.

PROBABLE CAUSE

5. In May 2012, personnel with the United States Army Corps of Engineers (USACE) in Cincinnati, Ohio, reported to U.S. Government security officials that XIAFEN CHEN, a Federal employee with the National Oceanic and Atmospheric Administration (NOAA) in Wilmington, Ohio, requested information on how the United States designs, builds, and operates reservoirs. The USACE employee became concerned because 1) the request was clearly outside the scope of CHEN's official duties, and 2) CHEN made the request in response to a prior request purportedly made by "Chinese colleagues".

6. Preliminary investigation by Special Agents from the U.S. Department of Commerce found that CHEN is a naturalized U.S. citizen of Chinese extraction. CHEN requested annual leave from approximately April 18, 2012 to May 8, 2012 to travel to the People's Republic of China (PRC). In approximately May 2012, while visiting family in the People's Republic of

China (PRC), CHEN was asked by her nephew TIAN RUI CHEN to meet with a PRC Government Official, to wit: Vice Minister of Water Resources YONG JIAO, under the auspice of assisting TIAN RUI CHEN's father-in-law with the resolution of a business dispute. CHEN agreed, and ultimately attended a meeting in JIAO's office. During the meeting, JIAO asked CHEN to provide information about how the U.S. repairs and maintains dams; shares the cost of dam projects; and what size dams belong to farmers and the government.

7. In furtherance of JIAO's request, CHEN, upon returning to the U.S., asked a co-worker at the NOAA facility in Wilmington, Ohio for his username and password to access the USACE National Inventory of Dams (NID) database portal. On approximately May 10, 2012, the coworker sent an email to CHEN containing his NID credentials and password via official NOAA email. CHEN never had any authorization from USACE or her NOAA supervisor to access the NID.

8. The National Inventory of Dams (NID) is a congressionally authorized database, which documents dams in the U.S. and its territories. The NID is maintained and published by USACE, in cooperation with the Association of State Dam Safety Officials (ASDSO), the states and territories, and federal dam-regulating agencies. The database contains sensitive and restricted information about the dams location, size, purpose, type, last inspection, regulatory facts, and other technical data. The information contained in the NID is updated approximately every two years.

9. The 2010 NID included information on approximately 84,000 dams of which 80 percent are regulated by the State Dam Safety Offices and almost 70 percent of the entire inventory is privately-owned dams. The federal government owns only 4% of the dam facilities listed in the NID, which includes approximately 40% of the tallest dams. From the 2010 NID, 13,990 dams

are classified as “high hazard potential”, 12,662 as “significant hazard potential”, 57,362 as “low hazard potential”, and 116 as “undetermined hazard potential”. Dams assigned the “high hazard potential” classification are those where failure or mis-operation will probably cause loss of human life. “Significant hazard potential” are those dams where failure or mis-operation results in no probable loss of human life but can cause economic loss. Dams assigned the “low hazard potential” classification are those where failure or mis-operation results in no probable loss of human life and low economic and/ or environmental losses. Losses are principally limited to the owner’s property. This hazard potential classification does not indicate the condition of the dam. There are approximately 2,000 more dams listed as “high hazard potential” than the previous NID.

10. The NID website enables query of dams using any of the 60+ fields of information, including dam name, height, type, purpose, year of construction, and owner, with query results shown on screen. Users can also display and query dams using the interactive map and show relevant features, such as state, county, congressional boundaries, waterways, and major cities. To query the database, users must first request an account from the NID website, located at <http://nid.usace.army.mil>. After a short approval process, users will receive an email notification with username and password.

11. An internet history review of CHEN’s official NOAA computer revealed that CHEN’s NOAA computer and login credentials were in fact used to access the NID database portal on the following approximate dates and times: May 10, 2012 from 2:30p.m. to 2:31 p.m.; May 11, 2012 from 11:29 p.m. to 11:29 p.m.; May 14, 2012 from 12:17 p.m. to 12:17 p.m.; and May 15, 2012 from 7:28 a.m. to 7:44 a.m.

12. Forensic analysis has revealed that on approximately May 10, 2012 at 2:37 p.m., CHEN's official NOAA computer and login credentials were used to download the file "OH.mdb" from the website <http://geo.usace.army.mil>. On May 15, 2012 at approximately 7:41 a.m., CHEN's official NOAA computer and login credentials were used to download the file "OH.mdb" from the website <http://geo.usace.army.mil>. These files are stored on the NID restricted and sensitive database.

13. USACE records revealed that CHEN was never an authorized NID user and did not have an active NID account. CHEN never obtained proper authorization from her NOAA supervisor to access the NID.

14. On May 15, 2012 at approximately 8:00 p.m., CHEN used her personal email account "XIAFENMAIL[[@YAHOO.COM](mailto:)]" to thereafter send an email to JIAO which included an overview of the information contained in the NID. In said email, CHEN states that the "database is only for government users and non-government users are not able to directly download any data from this site".

15. On May 29, 2012 at approximately 8:44 a.m., CHEN sent an email from her account "XIAFENMAIL[[@YAHOO.COM](mailto:)]" to JIAO indicating that she had spoken to the chief of the USACE Water Management Division. CHEN provided a summary of information to JIAO regarding the dams that USACE maintains; hydropower capacity; dam requirements; a link to USACE's mission page; and information on the future revision of policy and procedures for building new infrastructure.

16. On June 11, 2013, Special Agents from the US Department of Commerce personally interviewed CHEN about the above matter. During this interview, CHEN denied obtaining the

login credentials and password from her co-worker. CHEN also denied accessing the NID database and denied downloading information from the NID database.

17. The interviewing Agents thereafter presented CHEN with documentary evidence of the email sent to her by her co-worker containing the username and password to the NID database, as well as forensic data from CHEN's government computer showing the co-worker's username and password accessing the NID on four occasions.

18. After being confronted with this evidence, CHEN admitted to asking this co-worker for the username and password for the NID; receiving the username and password for the NID from this co-worker, and login credentials and password from her co-worker.

TECHNICAL BACKGROUND

19. In my training and experience, I have learned that YAHOO! provides a variety of online services, including electronic mail ("e-mail") access, to the general public. Subscribers obtain an account by registering with YAHOO!'s email service. During the registration process, YAHOO! asks subscribers to provide basic personal information. Therefore, the computers of YAHOO! are likely to contain stored electronic communications (including retrieved and un-retrieved email for YAHOO! subscribers) and information concerning subscribers and their use of YAHOO! services, such as account access information, email transaction information, and account application information.

20. In general, an email that is sent to a YAHOO! subscriber is stored in the subscriber's "mail box" on YAHOO! servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on YAHOO! servers indefinitely.

21. When a subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to YAHOO! servers, and then transmitted to its end destination. YAHOO! often saves a

copy of the email sent. Unless the sender of the email specifically deletes the email from the YAHOO server, the email can remain on the system indefinitely.

22. A YAHOO! subscriber can also store files, including emails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by YAHOO!.

23. Subscribers to YAHOO! might not store on their home computers copies of the emails stored on their YAHOO! account. This is particularly true when they access their YAHOO! account through the web, or if they do not wish to maintain particular emails or files in their residence.

24. In general, email providers like YAHOO! ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

25. Email providers typically retain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e. session) times and duration, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via YAHOO!'s website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

26. In some cases, email account users will communicate daily with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

27. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require YAHOO! to disclose to the government copies of the records and other information (including the content of communication) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. Disclosure of the sought after information is to be disclosed by YAHOO! without required notice to the subscriber/customer pursuant to 18 U.S.C. §2703(b)(1)(A).

CONCLUSION

28. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of YAHOO! there exists evidence of a crime and contraband or fruits of a crime. Accordingly a search warrant is requested.

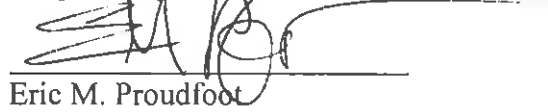
29. This court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation." 18 U.S.C. § 2703(a).

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING


31. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, e.g. by posting them publically on bulletin board forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Eric M. Proudfoot
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before
me this 12th day of June, 2014:


SHARON L. OVINGTON
UNITED STATES MAGISTRATE JUDGE
